Security Games with Partial Surveillance

(Extended Abstract)

Youzhi Zhang and Xudong Luo*
Institute of Logic and Cognition, Sun Yat-sen University, Guangzhou, 510275, China.
youzhi.zhang.lgc@gmail.com, luoxd3@mail.sysu.edu.cn

ABSTRACT

Security games are used to deploy limited security resources. Much work on the topic assumes that attackers have the perfect knowledge of defenders' strategies. However, it is not always the case in real life because an attacker may worry he will be caught if he observes defender's strategy on all targets. To address the issue, this paper proposes a new game model in which the attacker just selects partial targets to observe according to his goal and observation cost. Moreover, our theoretical and experimental analyses show that our model reflects well the way that attackers make decisions, and in particular, the defender can gain significantly higher utility by considering the attacker can only conduct observations on partial targets.

Categories and Subject Descriptors

I.2.11 [**Artificial Intelligence**]: Multiagent Systems

General Terms

Security, Theory

Keywords

Game theory, Security, Stackelberg games, Decision making

1. INTRODUCTION

Nowadays, the study of security games is very active [4, 6, 7, 1]. Generally speaking, in a security game, the defender needs to protect the people and critical infrastructure from the attacker. However, usually security resources are limited, and the attacker can observe the defender's security strategy for a period of time and then attack a target accordingly. So, the defender has to randomly cover all targets. That is, the defender should find an optimal mixed strategy to maximise his expected utility. The *strong Stackelberg equilibrium* [6] assumes that the attacker has the perfect knowledge of the defender's optimal strategy and accordingly chooses an optimal response strategy to maximise his expected utility.

*Corresponding author

Appears in: *Alessio Lomuscio, Paul Scerri, Ana Bazzan, and Michael Huhns (eds.), Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2014), May 5-9, 2014, Paris, France.*

However, very likely an attacker can observe the defender's mixed strategy on partial targets only. Actually, even though the more knowledge the attacker has may make his attack more successful, he also needs to reduce the observed target number to avoid the high observation cost (e.g., being detected and then caught by the defender). Therefore, the attacker can only have an ambiguous understanding of the defender's mixed strategy (the information for the unobserved part of targets is ambiguous). This is different from the assumption of typical Stackelberg games, i.e., the attacker has the perfect knowledge of the defender's strategy. Thus, it is required to model how the attacker selects targets to observe and accordingly chooses his optimal strategy.

Recently, much work has dealt with the imperfect observation in security games. Pita et al. [5] handle the attacker's limited observation on the defender's strategies with the bias toward the uniform probability distribution. Yin et al. [8] model the risk-averse strategies for the defender by considering the possible observations errors. An et al. [2, 1] propose models of limited surveillance where the attacker updates his belief based on the limited number of observations. In these models, the limited observation actually is some observations on all targets.

So, this paper models security games in the situation where the attacker just selects partial targets to observe based on his goal and observation cost along with an acceptability threshold. Then, in such a game, the attacker can only rely upon the ambiguous information about the defender's mixed strategy to determine his optimal strategy. We also investigate which factors can influence the process of the attacker's decision making and the defender's utility.

2. MODEL DEFINITION

Our model of Security Games with Partial Surveillance (SGPS) has the following sequence of moves. *Firstly*, the defender selects a mixed strategy. *Secondly*, the attacker selects partial targets to observe. After conducting such ambiguous observations, the attacker takes an optimal strategy based on his ambiguous belief about the defender's mixed strategy. Formally, we have:

Definition 1. A security games with partial surveillance (**SGPS**) is a tuple of (N, T, S, X, G, C, M, U), where:

1. $N = \{\boldsymbol{d}, \boldsymbol{a}\}$ is the set of players, where $\boldsymbol{d}$ stands for the defender and $\boldsymbol{a}$ stands for the attacker.
2. $T = \{t_1, \cdots, t_n\} = T_u \cup T_o$ with $T_u \cap T_o = \emptyset$ is the target set, where T_u is the set of unobserved targets and T_o is the set of observed targets by the attacker.

3. $S = S_{\boldsymbol{d}} \times S_{\boldsymbol{a}}$, where $S_{\boldsymbol{d}} = \{s_{\boldsymbol{d}}(t_1), \cdots, s_{\boldsymbol{d}}(t_n)\}$ and $S_{\boldsymbol{a}} = \{s_{\boldsymbol{a}}(t_1), \cdots, s_{\boldsymbol{a}}(t_n)\}$ are the pure strategy sets of the defender and the attacker, representing attacking or defending targets, and n is the target number.

4. $X = \{X_i \mid i = 1, \cdots, m\}$, where $X_i = \{p_{i,1}, \cdots, p_{i,n}\}$ is one mixed strategy of the defender, $p_{i,j}$ is the probability distribution for the pure strategy $s_{\boldsymbol{d}}(t_j)$ (satisfying $p_{i,j} \in [0,1]$ and $\sum_{p_{i,j} \in X_i} p_{i,j} = 1$).

5. $G = \{g_i \mid i = 1, \cdots, n\}$, where $g_i : t_i \rightarrow [0,1]$ is the attacker's goal satisfaction degree of target t_i.

6. $C = \{c_i \mid i = 1, \cdots, n\}$ where $c_i : t_i \rightarrow [0,1]$ is the observation cost when the attacker observes target t_i.

7. $M = \{m_i \mid i = 1, \cdots, m\}$, where m_i is the attacker's mass function over the target set T given the defender's mixed strategy X_i. More specifically, $\forall t_j \in T_o$, $m_i(\{t_j\}) = p_{i,j}$; and $m_i(T_u) = 1 - \sum_{t_j \in T_o} m_i(\{t_j\})$.

8. $U = \{(u_{\boldsymbol{d}}(s), u_{\boldsymbol{a}}(s)) \mid s \in S\}$, where $u_{\boldsymbol{d}}(s)$ and $u_{\boldsymbol{a}}(s)$ are the utility functions from strategy profile s to $\mathbb{R}$ for the defender and the attacker, respectively.

From the above definition, we can see that based on target t_i's goal satisfaction degree g_i and observation cost c_i, the attacker selects target set T_o to observe. Then, the information about the defender's strategy is ambiguous. That is, he only knows the covering probability of each observed target and the total covering probability $m_i(T_u)$ of the unobserved set of T_u because of the ambiguous observation. Thus, the attacker has to select the optimal response strategy based on this ambiguous information.

To get the attacker's optimal response strategy, the attacker needs to get the information about the defender's strategy. And then, the attacker needs to select some targets from all targets to observe based on his goal and his observation cost on each target. So, we use the acceptability function [3, 9] to define the observable degree with the attacker's acceptable threshold for each target to represent the degree that the attacker would like to observe the target. If the target could not satisfy that attacker's goal and the observation cost is too high, the attacker will not observe this target. However, if the reward of attacking a target is high, the attacker should consider more about this target. After observing the selected targets, the attacker has the ambiguous information about the defender's strategy. Based on this ambiguous information, the attacker finds the optimal response strategy using the D-S theory based decision model [10], i.e., the attacker gets the expected utility interval first, and then gets the point-valued expected utility based on the ambiguity degree of the information. Then, the defender can find his optimal strategy from his all mixed strategies.

3. INSIGHTS

Our theoretic analyses show some properties of our models as follows. First, if the observation cost is a constant for all targets, then the observed set is influenced by the goal satisfaction degrees more. Second, the attacker tries to avoid the target with the highest observation cost. Third, if there is a target in observed set T_o such that attacking it dominates the best strategy among all unobserved targets in T_u, the target that is the best for the attacker to attack must belong to the observed set of T_o.

Further, our experimental results reveals more insights into our model. First, the observed target number is decreasing with the acceptability threshold. Second, the attacker's utility increases with the observed target number. Third, as the number of observed targets increases, the defender's utility obtained by SGPS model is approaching to the utility obtained by SSE model. Fourth, SGPS is more robust than SSE model.

4. ACKNOWLEDGMENTS

This paper is supported by Bairen Plan of Sun Yat-sen University, Raising Program of Major Project of Sun Yat-sen University (No. 1309089), MOE Project of Key Research Institute of Humanities and Social Sciences at Universities (No. 13JJD720017) China, and China National Social Science Fund of Major Projects (13&ZD186).

5. REFERENCES

[1] B. An, M. Brown, Y. Vorobeychik, and M. Tambe. Security games with surveillance cost and optimal timing of attack execution. In *AAMAS*, pages 223–230, 2013.

[2] B. An, D. Kempe, C. Kiekintveld, E. Shieh, S. Singh, M. Tambe, and Y. Vorobeychik. Security games with limited surveillance. In *AAAI*, pages 1241–1248, 2012.

[3] X. Luo, N. R. Jennings, N. Shadbolt, H.-f. Leung, and J. H.-m. Lee. A fuzzy constraint based model for bilateral, multi-issue negotiations in semi-competitive environments. *Artificial Intelligence*, 148(1–2):53–102, 2003.

[4] J. Pita, M. Jain, J. Marecki, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus. Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport. In *AAMAS*, pages 125–132, 2008.

[5] J. Pita, M. Jain, M. Tambe, F. Ordóñez, and S. Kraus. Robust solutions to Stackelberg games: Addressing bounded rationality and limited observations in human cognition. *Artificial Intelligence*, 174(15):1142–1171, 2010.

[6] M. Tambe. *Security and game theory: Algorithms, deployed systems, lessons learned*. Cambridge University Press, New York, 2011.

[7] R. Yang, C. Kiekintveld, F. OrdóñEz, M. Tambe, and R. John. Improving resource allocation strategies against human adversaries in security games: An extended study. *Artificial Intelligence*, 195:440–469, 2013.

[8] Z. Yin, M. Jain, M. Tambe, and F. Ordónez. Risk-averse strategies for security games with execution and observational uncertainty. In *AAAI*, pages 758–763, 2011.

[9] Y. Zhang, X. Luo, and H.-f. Leung. Fuzzily constrained games. In *IAT*, volume 2, pages 361–368, 2013.

[10] Y. Zhang, X. Luo, and W. Ma. Security games with ambiguous information about attacker types. In *AI 2013*, volume 8272 of *LNCS*, pages 14–25. 2013.